PATENT OFFICE

JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: July 13, 2000

Application Number: Patent Application
No. 2000-212814

Applicant(s): FUJITSU LIMITED

December 22, 2000

Commissioner,
Patent Office Kozo Oikawa

Certificate No. 2000-3105869

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ７月１３日

出 願 番 号
Application Number: 特願２０００－２１２８１４

出 願 人
Applicant (s): 富士通株式会社

２０００年１２月２２日

特許庁長官
Commissioner,
Patent Office 及川耕造

【書類名】　特許願

【整理番号】　0051334

【提出日】　平成12年 7月13日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 15/00

【発明の名称】　Ｆｅｉｓｔｅｌ　構造とＳＰＮ構造とを組み合わせた演算装置および演算方法

【請求項の数】　7

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　下山　武司

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　伊藤　孝一

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　武仲　正彦

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　鳥居　直哉

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　矢嶋　純

出証特２０００－３１０５８６９

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　屋並　仁史

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　横山　和弘

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100074099

【住所又は居所】　東京都千代田区二番町８番地２０　二番町ビル３Ｆ

【弁理士】

【氏名又は名称】　大菅　義之

【電話番号】　03-3238-0031

【選任した代理人】

【識別番号】　100067987

【住所又は居所】　神奈川県横浜市鶴見区北寺尾７－２５－２８－５０３

【弁理士】

【氏名又は名称】　久木元　彰

【電話番号】　045-573-3683

【手数料の表示】

【予納台帳番号】　012542

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9705047

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　Feistel 構造とＳＰＮ構造とを組み合わせた演算装置および演算方法

【特許請求の範囲】

【請求項１】　データ入力を受け取り、該データ入力に対する演算結果をデータ出力とする演算装置において、

Feistel 構造を用いてデータ変換を行う第１のデータ変換手段の１つ以上と、

ＳＰＮ構造を用いてデータ変換を行う第２のデータ変換手段の１つ以上とが、前記データ入力とデータ出力との間で縦続的に組み合わされたことを特徴とするFeistel 構造とＳＰＮ構造とを組み合わせた演算装置。

【請求項２】　前記ＳＰＮ構造が、

前記データ入力の１ブロックのブロック長をワード長で除算した値の入・出力ビット数を持つ非線形変換手段と、

インタリーブ変換を用いる線形変換手段とを備えることを特徴とする請求項１記載のFeistel 構造とＳＰＮ構造とを組み合わせた演算装置。

【請求項３】　前記ＳＰＮ構造を構成する非線形変換手段として、

該非線形変換手段への入力ビットのうちで固定された１つ以上の入力ビットにのみ差分が与えられた入力データの組に対して、前記固定された１つ以上の入力ビットと同じ位置にある固定された１つ以上の出力ビットにのみ出力データの組に差分が現われる確率が０となり、

かつ該固定された１つ以上の入力ビット、および該固定された１つ以上の出力ビットにのみ関係する任意の線形関係式がすべての入・出力データ間で成立する確率が１／２となる非線形変換手段を備えることを特徴とする請求項１、または２記載のFeistel 構造とＳＰＮ構造とを組み合わせた演算装置。

【請求項４】　データ入力を受け取り、該データ入力に対する演算結果をデータ出力とする演算方法において、

Feistel 構造を用いてデータ変換を行う第１のデータ変換ステップの１つ以上と、

ＳＰＮ構造を用いてデータ変換を行う第２のデータ変換ステップの１つ以上と

を、前記データ入力とデータ出力との間で組み合わせて実行することを特徴とするFeistel 構造とＳＰＮ構造とを組み合わせた演算方法。

【請求項５】　前記ＳＰＮ構造を用いる第１のデータ変換ステップにおいて、

前記データ入力の１ブロックのブロック長をワード長で除算した値を入・出力ビット数とする非線形変換と、

インタリーブ変換を用いる線形変換とを実行することを特徴とする請求項４記載のFeistel 構造とＳＰＮ構造とを組み合わせた演算方法。

【請求項６】　前記ＳＰＮ構造内で実行されるべき非線形変換として、

該非線形変換においての入力ビット数のうちで固定された１つ以上の入力ビットにのみ差分が与えられた入力データの組に対して、前記固定された１つ以上の入力ビットと同じ位置にある固定された１つ以上の出力ビットにのみ出力データの組に差分が現われる確率が０となり、

かつ該固定された１つ以上の入力ビット、および該固定された１つ以上の出力ビットにのみ関係する任意の線形関係式がすべての入・出力データ間で成立する確率が１／２となる非線形変換を実行することを特徴とする請求項４、または５記載のFeistel 構造とＳＰＮ構造とを組み合わせた演算方法。

【請求項７】　データ入力を受け取り、該入力データに対する演算結果をデータ出力とする演算を実行する計算機によって使用される記憶媒体において、

Feistel 構造を用いてデータ変換を行う第１のデータ変換ステップの１つ以上と、

ＳＰＮ構造を用いてデータ変換を行う第２のデータ変換ステップの１つ以上とを、前記データ入力とデータ出力との間で組み合わせて実行させる機能を備えるプログラムを格納した計算機読出し可能可搬型記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は共通鍵ブロック暗号方式に係り、更に詳しくはFeistel 構造とＳＰＮ構造とを組み合わせ、かつＳＰＮ構造に特別の工夫を行ってデータの拡散性を向

上させる暗号化装置、および暗号化方法に関する。

【０００２】

【従来の技術】

高度情報化社会を迎え、情報セキュリティの確保は緊急の課題となっている。情報セキュリティの基本となるのはデータの暗号化である。高度情報化社会において高速、かつ安全な通信を実現するために共通鍵ブロック暗号は不可欠の技術である。この共通鍵ブロック暗号のアルゴリズムとして従来様々な方式が提案されているが、それらは基本的にはFeistel 構造と呼ばれる構造の繰返しか、あるいはＳＰＮ構造と呼ばれる構造の繰返しのいずれかであった。

【０００３】

図１２はFeistel 構造の説明図である。同図において、例えば入力１２８ビットは右側６４ビットと左側６４ビットに分割され、右側６４ビットはＦ関数５１と呼ばれる非線形関数に入力され、その出力と左側６４ビットとがＸＯＲ５２によって排他的論理和がとられ、その結果が出力１２８ビットのうちの右側６４ビットとして出力され、左側６４ビットとしては入力１２８ビットのうちの右側６４ビットがそのまま出力される。このようなFeistel 構造が、例えば１６段繰り返されて、暗号化が行われる。

【０００４】

図１３はＳＰＮ構造の例である。この構造においては、Ｓボックスと呼ばれる非線形変換５３と、線形変換Ｐ５４とが組み合わされて用いられる。

ＳボックスのＳはサブスティテューション、すなわち換字を、関数Ｐはパーミュテーション、すなわち置換を意味するが、現在ではＳはより一般的に非線形写像を、またＰは置換だけではなく、ビット単位の線形変換を指すものとなっている。

【０００５】

いずれにせよ、このようなＳＰネットワーク（ＳＰＮ）構造が多段に繰り返されることによって暗号化が行われる。なお図１２のFeistel 構造内のＦ関数として後述するようにＳＰＮ構造が用いられるが、図１２は全体としてはFeistel 構造を示すものである。

【０００６】

【発明が解決しようとする課題】

以上のような共通鍵ブロック暗号方式においては、Feistel 構造、ＳＰＮ構造のいずれを用いるとしても、なるべく少ない段数でデータの安全性が保証されるような暗号化を行う必要がある。しかしながら、まずFeistel 構造を用いる場合には１段で入力データ長の半分しか攪拌されず、ワード内のデータ攪拌には効果があるが、ワードを越えたデータ攪拌能力が劣るという問題点がある。また入出力が対称の形式となっていることから、暗号としては繰返し型の差分近似式、または線形近似式が存在する可能性があり、差分攻撃や線形攻撃にさらされる危険性があるという問題点があった。

【０００７】

これに対してＳＰＮ構造を用いる場合には、ワード間のデータ攪拌性には効果があり、入出力が非対称の形式であるという長所を持つが、入力データ長全体を分割して複数のＳボックスに入力させる必要があり、Ｓボックスは一般にメモリ内にテーブルとして保持されるものを使用するため、Ｓボックスの数が増えることによってテーブル参照回数が増加し、ＳＰＮ構造だけを何段も組み合わせる場合には、処理に時間がかかるという問題点があった。

【０００８】

本発明の課題は、上述の問題点に鑑み、Feistel 構造とＳＰＮ構造とを組み合わせてそれぞれの欠点をできるだけ解消させる暗号化を行うと共に、ＳＰＮ構造内のＳボックスにおいてもデータ攪拌効果を更に向上させることによって、演算量をできるだけ削減し、かつデータ拡散性能に優れた暗号化装置、および暗号化方法を提供することである。

【０００９】

【課題を解決するための手段】

図１は本発明の演算装置の原理構成ブロック図である。同図はデータ入力を受け取り、そのデータ入力に対する演算結果をデータ出力とする演算装置を示す。この演算装置１では、Feistel 構造を用いてデータ変換を行う第１のデータ変換手段２の１つ以上と、ＳＰＮ構造を用いてデータ変換を行う第２のデータ変換手

段３の１つ以上とが、データ入力とデータ出力との間で縦続的に組み合わされる。

【００１０】

図１（ａ）においては、データ入力に対して最初に第１データ変換手段２、次に第２のデータ変換手段３が用いられ、（ｂ）においては逆に最初に第２のデータ変換手段３が、次に第１のデータ変換手段２が用いられる。

【００１１】

（ｃ）においては先ず第１のデータ変換手段２が２段用いられた後に、第２のデータ変換手段３が用いられる。（ｄ）においては逆に第２のデータ変換手段３が用いられた後に、第１のデータ変換手段２が２段連続に用いられてデータ出力が行われる。

【００１２】

このように本発明においては第１のデータ変換手段２の１つ以上と、第２のデータ変換手段３の１つ以上とが組み合わされて用いられるが、Feistel 構造を用いる第１のデータ変換手段２については、１段ではデータの片側しか攪拌されないため、例えば２段連続的に用いられてデータの両側の攪拌が行われるような形式で組み合わせが行われる。なお、２つのデータ変換手段をさらに多数組み合わせることも当然可能である。

【００１３】

本発明の実施の形態においては、ＳＰＮ構造の中にデータ入力の１ブロックのブロック長、例えば１２８ビットをワード長３２ビットで割算した値、例えば４ビットの入・出力ビット数を持つ非線形変換手段、例えばＳボックスと、インタリーブ変換を用いる線形変換手段とを備えることもできる。

【００１４】

また発明の実施の形態においてはＳＰＮ構造を構成する非線形変換手段、例えばＳボックスとして入力ビット数、例えば４ビットのうちで、１つ以上、例えば右側２ビットにのみ差分が与えられた入力データの組に対して、同じ位置、すなわち右側２ビットにのみ出力データの組に差分が現われる確率が０となり、かつ例えば右側２ビットの入力ビットおよび右側２ビットの出力ビットにのみ関係す

る任意の線形関係式がすべての入出力データ間で成立する確率が１／２となる非線形変換手段を備えることもできる。

【００１５】

本発明の演算方法においては、データ入力に対する演算結果をデータ出力とする演算方法において、Feistel 構造を用いてデータ変換を行う第１のデータ変換ステップの１つ以上と、ＳＰＮ構造を用いてデータ変換を行う第２のデータ変換ステップの１つ以上とを、データ入力とデータ出力の間で組み合わせて実行する演算方法が用いられる。

【００１６】

発明の実施の形態においては、この演算方法内のＳＰＮ構造を用いた第１のデータ変換ステップにおいて、データ入力の１ブロックのブロック長をワード長で割った値を入出力ビット数とする非線形変換と、インタリーブ変換を用いる線形変換とを実行することもできる。

【００１７】

また本発明の実施の形態においては、このＳＰＮ構造内で実行されるべき非線形変換として、入力ビット数のうちで１つ以上、例えば右側半数の入力ビットにのみ差分が与えられた入力データの組に対して、同じ右側半数の出力ビットにのみ出力データの組に差分が現われる確率が０となり、かつ右側半数の入力ビット、および右側半数の出力ビットにのみ関係する任意の線形関係式がすべての入・出力データの間で成立する確率が１／２となる非線形変換を実行することもできる。

【００１８】

更に本発明においては、データ入力を受け取り、そのデータ入力に対する演算結果をデータ出力とする演算を実行する計算機によって使用される記憶媒体として、Feistel 構造を用いてデータ変換を行う第１のデータ変換ステップの１つ以上と、ＳＰＮ構造を用いてデータ変換を行う第２のデータ変換ステップの１つ以上とを、データ入力とデータ出力との間で組み合わせて実行させる機能を有するプログラムを格納した計算機読出し可能可搬型記憶媒体が用いられる。

【００１９】

以上のように本発明によれば、Feistel 構造とＳＰＮ構造とがデータ入力とデータ出力との間で組み合わされて演算が実行され、更にＳＰＮ構造の内部で、例えば右側半数の入力ビットにのみ差分が入力データの組に現われた場合、右側半数の出力ビットには出力データの組に差分が現われないような非線形変換が用いられる。

【００２０】

【発明の実施の形態】

本発明においては、Feistel 構造とＳＰＮ構造とが組み合わされて、演算装置、または演算方法が構成されるが、そのような演算装置および演算方法として、入力された平文を暗号化して出力する暗号文生成装置、および生成方法を発明の実施形態として説明する。

【００２１】

図２はそのような暗号文生成装置のシステム構成ブロック図である。同図において、暗号文生成装置は処理装置１０、入力ファイル１１、出力ファイ１２、表示装置１３、および入出力装置１４によって構成されている。

【００２２】

処理装置１０の内部には、使用されるFeistel 構造を決定するFeistel 構造決定部１６、ＳＰＮ構造を決定するＳＰＮ構造決定部１７、Feistel 構造とＳＰＮ構造とを組み合わせた暗号化アルゴリズムを決定する暗号化アルゴリズム決定部１８、その暗号化アルゴリズムに従って平文を暗号化する暗号文生成部１９を備えている。

【００２３】

入力ファイル１１には暗号化されるべき入力データとしての平文、入力データ１ブロックのビット長ｎ、処理装置１０による演算に適当なワードのビット長ｗ、および後述するようにＳＰＮ構造の中で用いられる線形変換としてのインタリーブ変換の内容などが格納されている。

【００２４】

また出力ファイル１２には、Feistel 構造決定部１６によって決定されるFeistel 構造に用いられているＦ関数、ＳＰＮ構造決定部１７によって決定されるＳ

ボックスの非線形関数に相当する写像Ｓ、および暗号化アドレス決定部１８によって決定されたFeistel 構造とＳＰＮ構造の組合せとしての暗号化アルゴリズムなどが格納される。

【００２５】

図３は本実施形態におけるFeistel 構造とＳＰＮ構造との組合せ、すなわち暗号化アルゴリズム決定部１８によって決定された暗号化アルゴリズムの例である。同図において、入力データに対してまずFeistel 構造２０ａ、２０ｂによる演算が２段行われる。その後ＳＰＮ構造２３による演算が行われ、その結果に対して更に２段のFeistel 構造２０ｃ，２０ｄによる演算が行われ、その結果が暗号文として出力されることになる。

【００２６】

図３においては、１段のFeistel 構造によっては入力データのうち片側半分しか攪拌されないため、Feistel 構造が２段重ねて用いられると共に、後述するようにＳＰＮ構造２３にワード内の攪拌効果を大きくする工夫が取り入れられる。すなわちＳボックスで用いられる非線形関数に対して、後述する図８、図９のような性質を持つ関数を用いてワード内の攪拌効果を大きくすると共に、更に線形変換としてインタリーブ変換を用いることによって、１つのブロックを構成する複数のワードの間での攪拌効果が大きくなるようにＳＰＮ構造が構成される。

【００２７】

なお、Feistel 構造を３段以上連続して用いるとＳＰＮ構造を組み合わせた効果が薄れてくるため、図３ではＳＰＮ構造が２段のFeistel 構造の間に挿入された組合せとなっている。

【００２８】

図４はそのＳＰＮ構造２３の概略の説明図である。同図において入力データ、例えば１２８ビットに対してまずインタリーブ変換２４が行われ、例えば３２ビットで構成される４つのワード間のデータの攪拌が行われる。その攪拌結果は複数のＳボックス２５に与えられ、Ｓボックス２５の出力に対してインタリーブ逆変換２６が行われて、ＳＰＮ構造の出力となる。

【００２９】

図５は本実施形態における暗号文生成処理の全体フローチャートである。同図において処理が開始されると、まずステップＳ１で平文、すなわち入力データブロックのビット長ｎが入力されて、ステップＳ２でFeistel 構造Ｒが定められる。本実施形態においては、このFeistel 構造内の非線形関数Ｆとして任意の関数を用いることができるものとするが、その例については図６で説明する。

【００３０】

続いてステップＳ３で演算器に適するワードのビット長ｗが入力され、ステップＳ４でＳＰＮ構造Ｂが定められる。このＳＰＮ構造Ｂについては、図４で説明したようにインタリーブ変換とＳボックスの非線形関数の内容が問題となるが、これらについては後述する。

【００３１】

そしてステップＳ５で、１段以上のFeistel 構造と１段以上のＳＰＮ構造とが組み合わされて、例えば図３で示したような暗号化アルゴリズムが定められ、ステップＳ６でその暗号化アルゴリズムに従って入力データとしての平文が暗号化されて暗号文が生成され、処理を終了する。

【００３２】

図６は本実施形態においてFeistel 構造の内部で用いられるＦ関数の例である。このＦ関数としては、前述のように任意の非線形関数を用いることができ、その意味でＦ関数として図６のものを用いなければならない理由はないが、その構成について特徴的な部分を中心に説明する。

【００３３】

図６において、入力データ６４ビットはそれぞれ右側、左側３２ビットずつに分割され、ＸＯＲ３０ａ，３０ｂによってｋｅｙ１とｋｅｙ２との排他的論理和がそれぞれとられ、６ビットまたは５ビットずつに分割されて、それぞれ６つのＳボックス３１に入力される。一般的にはＳボックスとして全てのＳボックスの入出力ビット数が等しいものを並べて使う場合が多い。ここでは６ビット入出力のＳボックスと５ビットの入出力のＳボックスとを混在させて用いているが、その詳細については説明を省略する。

【００３４】

それぞれ６個のＳボックス３１の出力はＭＤＳ変換部３２ａ，３２ｂに与えられる。ここでＭＤＳ変換部は、図１２で説明したＳＰＮ構造における関数Ｐに相当し、その意味ではFeistel 構造内のＦ関数はＳＰＮ構造を持つともいえるが、このＰ関数におけるデータの拡散性を定義する１つの概念としての分岐数を最大とする線形変換層がＭＤＳ変換部である。この分岐数は、暗号に対する差分攻撃や、線形攻撃に対する強度を評価するバロメータであり、その詳細については次の文献で説明されている。

文献）共通鍵ブロック暗号の選択／設計／評価に関するドキュメント、通信・放送機構

ＭＤＳ変換部３２ａ，３２ｂの出力は、それぞれＸＯＲ３３ａ，３３ｂに与えられ、排他的論理和がとられるが、例えばＭＤＳ変換部３２ａの出力３２ビットに対しては、Ｏｘ５５５５　５５５５との論理積がとられた後にＥｘオア３３ｂに与えられる。このような論理積がとられるのは、ＭＤＳ変換部３２ａ，３２ｂの出力がそのまま与えられるのでは、Ｅｘオア３３ａ，３３ｂの出力は同じになってしまうためである。ここでＭＤＳ変換部３２ａの出力と論理積がとられるデータは２進数では０１０１０１・・・０１０１（３２ビット）であり、またＭＤＳ変換部３２ｂの出力と論理積がとられるデータは１０１０１０・・・１０１０（３２ビット）である。

【００３５】

図７は図５のステップＳ４、すなわちＳＰＮ構造Ｂの決定処理の詳細フローチャートである。同図において処理が開始されると、まずステップＳ９で入出力ビット数が求められた後に、ステップＳ１０でランダムな写像Ｓが新しく選択される。この写像Ｓは、図５のステップＳ１で入力されたブロックのビット長ｎを、ステップＳ３で入力されたワードのビット長ｗで割った結果としての、ｒビット入出力の１対１写像である。

【００３６】

例えば平文、すなわち入力データのブロックのビット長ｎが１２８ビットであり、ワード長ｗが３２ビットであるとすると、ｒは４ビットとなり、４ビット入出力のランダムな写像Ｓが選択される。

【００３７】

図７のステップＳ１１で、写像Ｓを対象として固定された半数の入力ビット、例えば４ビットのうち２ビットにのみ差分が与えられた入力データの組に対して、同じ位置にある固定された半数の出力ビットにのみ出力データの組に差分が現われる確率が０であるか否かが判定され、０でない場合にはステップＳ１０に戻り、新しいランダムな写像Ｓの選択以降の処理が繰り返される。

【００３８】

ステップＳ１１で確率が０と判定されると、ステップＳ１２で写像Ｓを対象として固定された半数の入力ビット、および例えば同じ位置にある固定された半数の出力ビットのみに関係する任意の線形関係式について、全ての入出力ビットデータ間でその線形関係式が成立する確率が１／２であるか否かが判定され、１／２でない場合にはステップＳ１０以降の処理が繰り返される。なおステップＳ１１、Ｓ１２における判定については図８、図９を用いて更に後述する。

【００３９】

ステップＳ１２で確率が１／２である場合には、ステップＳ１３でその写像Ｓとインタリーブ変換、例えば図１０で後述するインタリーブ変換であって、図２の入力ファイル１１に格納されているインタリーブ変換とが組み合わされてＳＰＮ構造Ｂが定められ、処理を終了する。

【００４０】

図８は図７のステップＳ１１で判定される確率の例である。この例は、４ビットを入出力ビット数とする非線形のＳ関数として

Ｓ：（０，１，２，３，４，５，６，７，８，９，10，11，12，13，14，15）
→（１，９，６，12，７，２，15，11，14，０，５，10，４，３，８，13）

の関数を用いた場合の例であり、入力差分に対して出力差分が現われる確率としてのｘ／１６のｘを表わしたものである。なおこの非線形Ｓ関数の入出力関係において、例えば最後の10進１５に対して10進１３が出力されること、すなわち２進数１１１１に対して１１０１が出力されることが示されている。

【００４１】

図８において４ビットのうち右側半分に入力差分が表われている上の３行にお

いては、対応する位置の片側半分に出力差分が現われる確率、すなわち左側３列の確率は０であることが、また左側半分に入力差分が現われている入力データの組、すなわち下側３行に対しては左側半分に出力差分が現われる確率、すなわち右側３列の確率が０であることが示されている。

【００４２】

図８において、例えば入力差分が（０００１）であり、かつ出力差分が（０１００）である入出力データ組は入力組（０１１０），（０１１１）に対する出力組（１１１１），（１０１１）と、入力組（０１１１），（０１１０）に対する出力組（１０１１），（１１１１）の２組だけであることが計算によって確認されている。

【００４３】

図９は図７のステップＳ１２で判定される確率の例を示す。この確率は前述の非線形Ｓ関数に対する確率を示すものである。すなわち、片側２入力ビットおよび片側２出力ビットのみに関係した任意の全ての線形関係式について、全入出力ビットデータ間でその線形関係式が成立する確率（８－ｘ）／１６を決めるｘを示すものである。

【００４４】

図９において、右側２入力ビットと右側２出力ビットとにそれぞれ差分が現われるのは上３行の左側３列であり、このような入出力ビットデータ間で線形関係式が成立する確率を示すｘの値が０であることから、その確率は８／１６，すなわち１／２となる。

【００４５】

同様に左側２入力ビット、左側２出力ビットに差分が現われるのは、下３行のうち右側３列であり、これらの入出力データ間においても線形関係式の成立確率は１／２となる。線形関係式の成立確率が１／２となるということは、その入出力データ間でその線形関係式が成立することもあり、また成立しないこともあることを示し、その線形関係式自体に意味がないことを示している。

【００４６】

入出力ビットに関するある線形式の値が常に０、または１となるとき、入出力

の間にその線形式が成立することになる。暗号においては入出力が線形関係からできるだけ離れていることが望ましく、その意味で前述の成立確率１／２という状況が望ましい。

【００４７】

入力を（x_0，x_1，x_2，x_3）、出力を（y_0、y_1，y_2，y_3）とし、入力（０００１）、出力（０１００）に関係する線形式$x_3 + y_1$の値を調べることにする。前述の写像Ｓで入力１＝（０００１）に対する出力は９＝（１００１）であることから、$x_3 + y_1 = 1 + 0 = 1$となる。同様にして、すべての入出力の間で$x_3 + y_1$の値は次のように求められる。

【００４８】

Ｉｎ０，Ｏｕｔ１→０

Ｉｎ１，Ｏｕｔ９→１

Ｉｎ２，Ｏｕｔ６→１

Ｉｎ３，Ｏｕｔｃ→０

Ｉｎ４，Ｏｕｔ７→１

Ｉｎ５，Ｏｕｔ２→１

Ｉｎ６，Ｏｕｔｆ→１

Ｉｎ７，Ｏｕｔｂ→１

Ｉｎ８，Ｏｕｔｅ→１

Ｉｎ９，Ｏｕｔ０→１

Ｉｎａ，Ｏｕｔ５→１

Ｉｎｂ，Ｏｕｔａ→１

Ｉｎｃ，Ｏｕｔ４→１

Ｉｎｄ，Ｏｕｔ３→１

Ｉｎｅ，Ｏｕｔ８→０

Ｉｎｆ，Ｏｕｔｄ→０

この計算によって、$x_3 + y_1 = 1$という線形式が成立する入出力関係は１２となり、確率が１２／１６となることから図９内で対応するｘの値は－４となる。

【００４９】

図１０は図４で説明したインタリーブ変換の例である。同図において、例えばＳＰＮ構造への入力データは、Ａ，Ｂ，Ｃ，Ｄの４つの部分に分割され、分割されたデータは４行で示されるような形式に変換される。更にＡ，Ｂ，Ｃ，Ｄのデータが列に並ぶように変換され、最終的にＡ，Ｂ，Ｃ，Ｄのデータのうちの最初の部分が１番目に並べられ、次の部分が２番目に、以下同様に並べられるような形式に変換されて、例えばＡ，Ｂ，Ｃ，Ｄの最初の部分、すなわち１番目に並べられたデータが、図４で最も左側にあるＳボックス２５に入力されることになる。

【００５０】

例えばＡを３２ビット変数Ｘ，ＢをＹ，ＣをＺ，ＤをＷ（それぞれ３２ビット変数）に割り当て、$X=(x_0, x_1, \cdots x_{31})$，$Y=(y_0, y_1, \cdots y_{31})$，$Z=(z_0, z_1, \cdots z_{31})$，$W=(w_0, w_1, \cdots w_{31})$とすると、図１０のインタリーブ変換の出力は$(x_0, y_0, z_0, w_0, x_1, y_1, z_1, w_1, \cdots x_{31}, y_{31}, z_{31}, w_{31})$となる。

【００５１】

このように本実施形態においては、非線形Ｓ関数と、線形変換としてのインタリーブ変換とを組み合わせることによって、入力データの攪拌性能の向上が図られる。

【００５２】

図８、図９で説明したように、Ｓボックスの入力の片側２ビット、例えば右側２ビットに入力差分が与えられた時、右側２ビットに出力差分が現われる確率は０であり、左側２ビットに出力差分が現われる確率が０とならないことから、右側半分に差分が与えられた入力データの組に対しては左側にその影響が現われることになり、データの攪拌効果が得られる。

【００５３】

図９では右側２ビットの入力ビットと出力ビットのみに関係する線形関係式の成立確率が１／２となる。すなわちその線形関係式に意味がないのに対して、右側２ビットと左側２ビットのみに関係した線形関係式については、その成立確率

が１／２より大きくなるものが明らかに存在することになる。右側２ビットと左側２ビットとを関係づける線形関係式によってデータの攪拌効果が得られることになる。

【００５４】

図１１は本実施形態におけるプログラムのコンピュータへのローディングの説明図である。本発明の実施形態としての暗号化装置、例えば図２に示したシステムなどは、当然一般的なコンピュータシステムによって構成することができる。図１１はそのようなシステムの構成を示し、コンピュータ４１は本体４２とメモリ４３とによって構成されている。メモリ４３はランダムアクセスメモリ（ＲＡＭ）、ハードディスク、磁気ディスクなどの記憶装置であり、本発明の特許請求の範囲第７項のプログラムや、図５、図７で説明したプログラムなどはメモリ４３に格納され、そのプログラムが本体４２によって実行されることによって、本発明の演算方法が実現され、入力データに対する暗号化が行われる。

【００５５】

本発明を実現するためのプログラムは、プログラム提供者側からネットワーク４４を介してコンピュータ４１にロードされることも、また市販され、流通している可搬型記憶媒体４５に格納され、そのプログラムがコンピュータ４１にロードされることによって実現されることも可能である。可搬型記憶媒体４５としてはフロッピィディスク、ＣＤ－ＲＯＭ、光ディスク、光磁気ディスクなど様々な形式の記憶媒体を使用することができ、前述のプログラムなどがこのような記憶媒体に格納され、コンピュータ４１にロードされることによって、本実施形態における暗号化アルゴリズムが出力され、その暗号化アルゴリズムを用いて入力データに対する暗号文を生成することが可能となる。

【００５６】

【発明の効果】

以上詳細に説明したように、本発明によればワード内でのデータの攪拌、および拡散性能に優れたFeistel 構造と、ワード間の攪拌性や、高速演算性、入出力についての非対称性などの性質を持つＳＰＮ構造とを組み合わせることによって、暗号化演算の高速性を図ると共に、暗号の安全性を向上させることができる。

更にＳＰＮ構造におけるＳブロックの非線形関数として、データの攪拌がデータの片側に偏らないような写像を用いることによりデータ攪拌性を向上させると共に、インタリーブ変換を用いることによってワード間のデータの攪拌性を更に向上させることができ、共通鍵ブロック暗号の性能向上に寄与するところが大きい。

【図面の簡単な説明】

【図１】

本発明の原理構成ブロック図である。

【図２】

本発明における暗号化装置のシステム構成ブロック図である。

【図３】

Feistel 構造とＳＰＮ構造の組合せの例を示す図である。

【図４】

ＳＰＮ構造の構成例を示す図である。

【図５】

暗号化アルゴリズムの決定と入力データの暗号化処理の全体処理フローチャートである。

【図６】

Feistel 構造で用いられるＦ関数の例を示す図である。

【図７】

ＳＰＮ構造決定処理の詳細フローチャートである。

【図８】

Ｓ関数に与えられる入力差分に対して出力差分が現われる確率を説明する図である。

【図９】

Ｓ関数における入出力ビットの間の線形関係式の成立確率を説明する図である。

【図１０】

インタリーブ変換の例を説明する図である。

【図１１】

プログラムのコンピュータへのローディングを説明する図である。

【図１２】

Feistel 構造の例を示す図である。

【図１３】

ＳＰＮ構造の例を示す図である。

【符号の説明】

１　演算装置

２　第１のデータ変換手段

３　第２のデータ変換手段

１０　処理装置

１１　入力ファイル

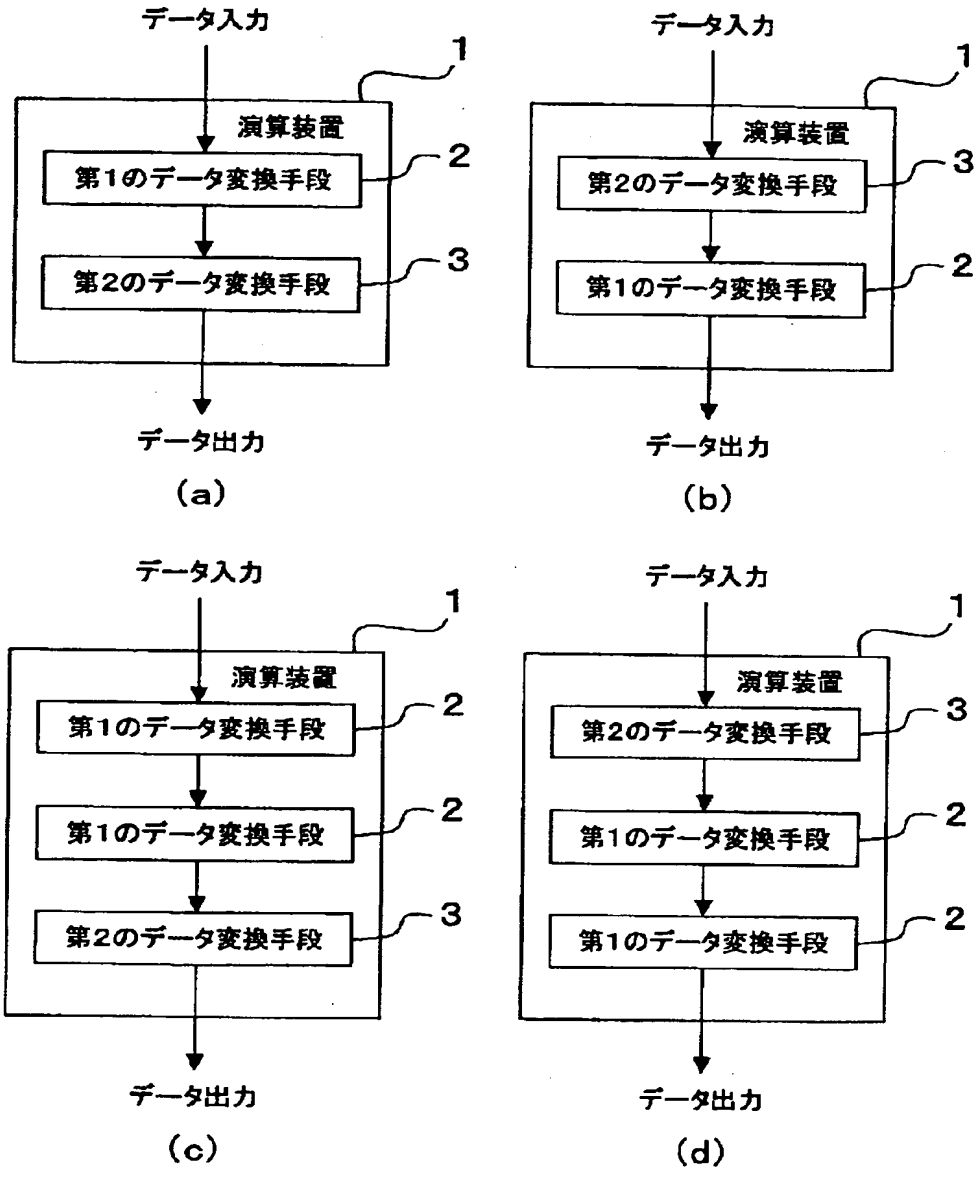
１２　出力ファイル

１３　表示装置

【書類名】　　図面

【図１】

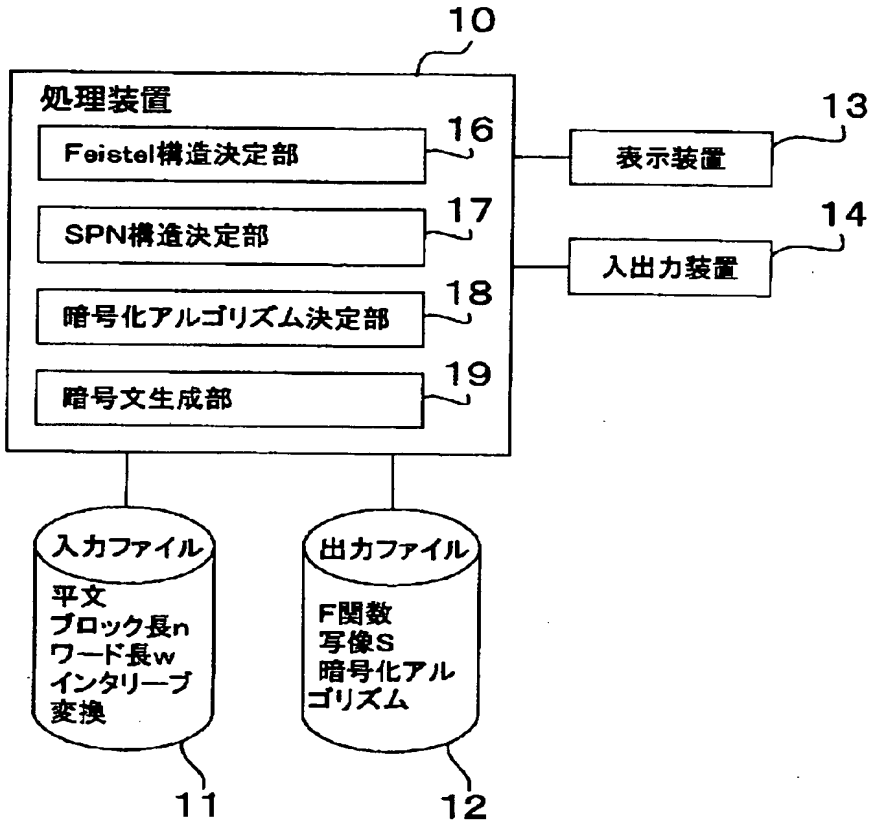
本発明の原理構成ブロック図



出証特２０００－３１０５８６９

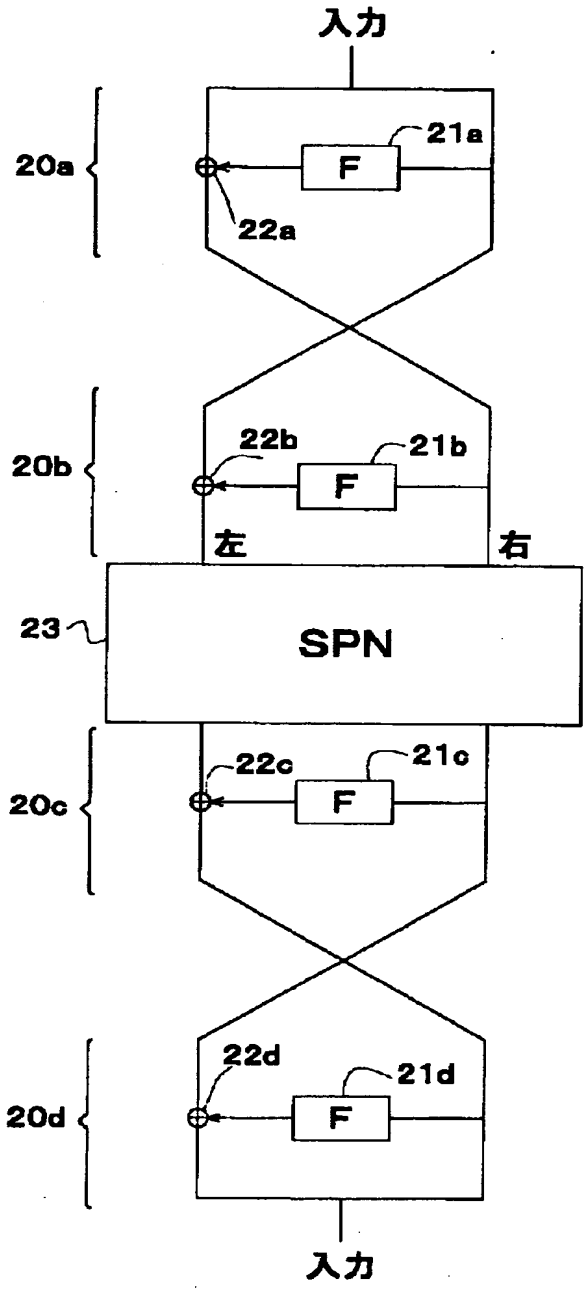
【図２】

本発明における暗号化装置のシステム構成ブロック図



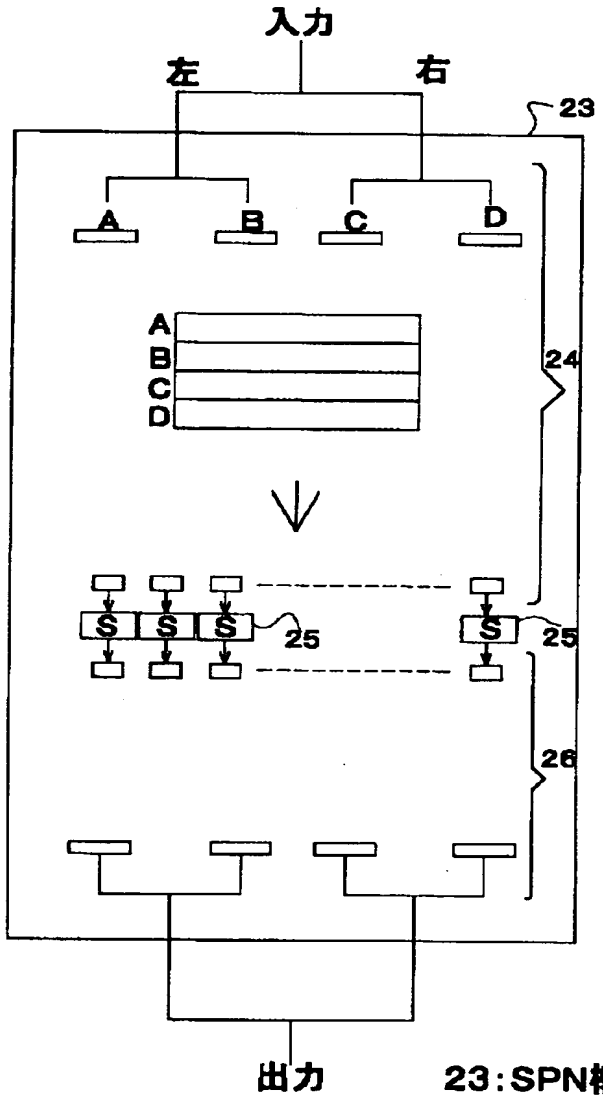
【図３】

Feiste1構造とSPN構造の組合わせの例を示す図



【図４】

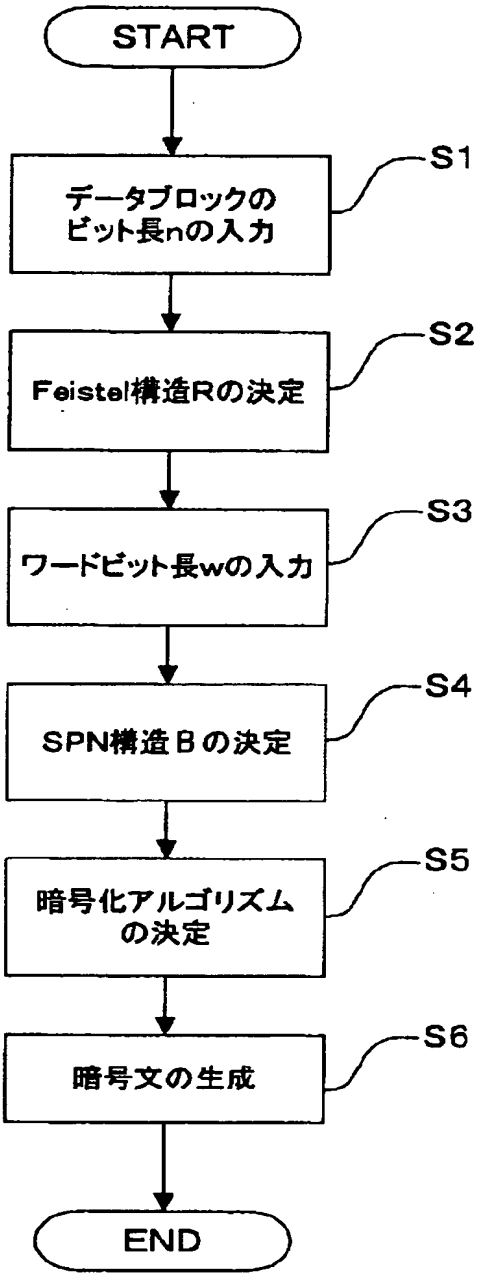
SPN構造の構成例を示す図



23:SPN構造
24:インターリーブ変換
25:Sボックス
26:インターリーブ逆変換

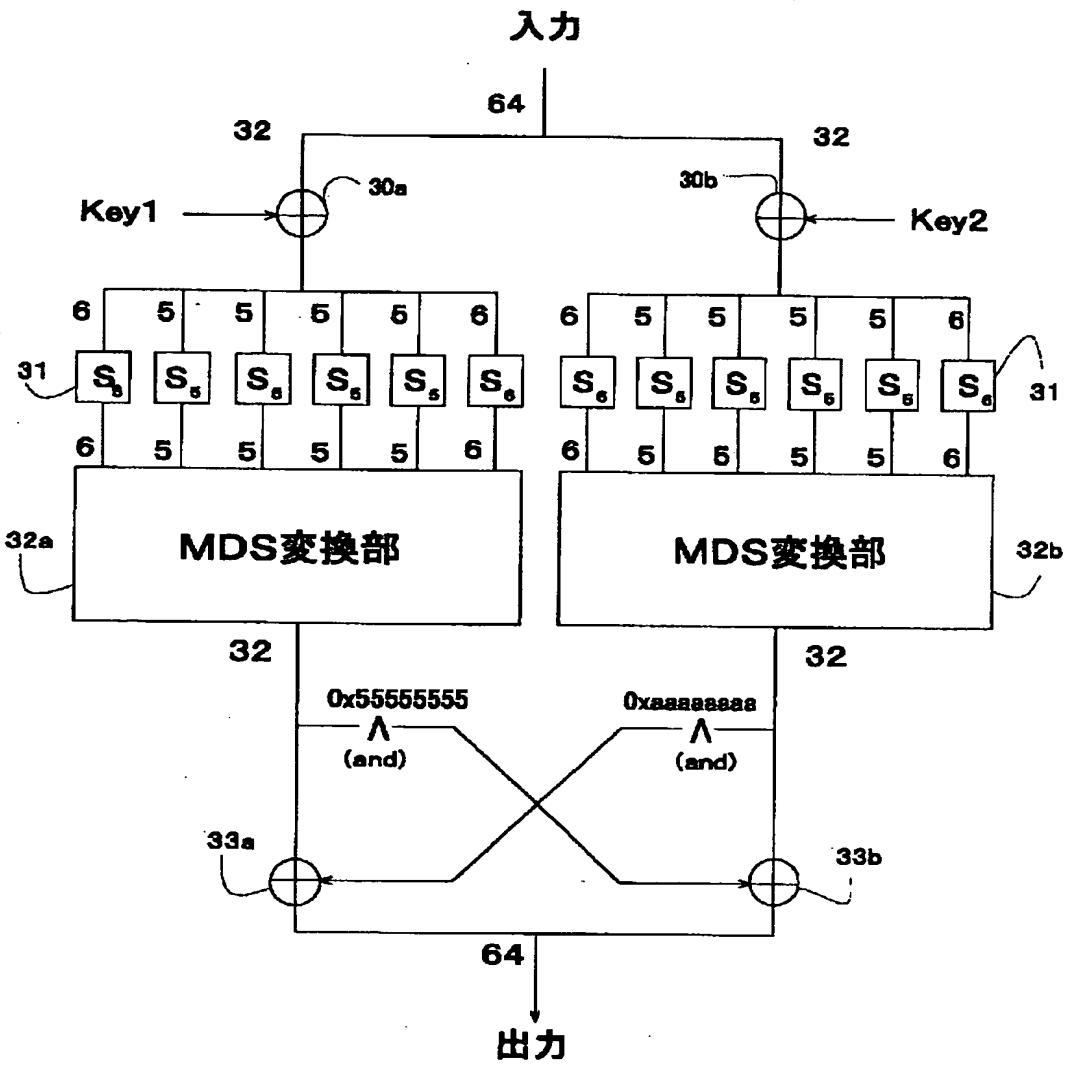
【図５】

暗号化アルゴリズムの決定と
入力データの暗号化処理の全体処理フローチャート



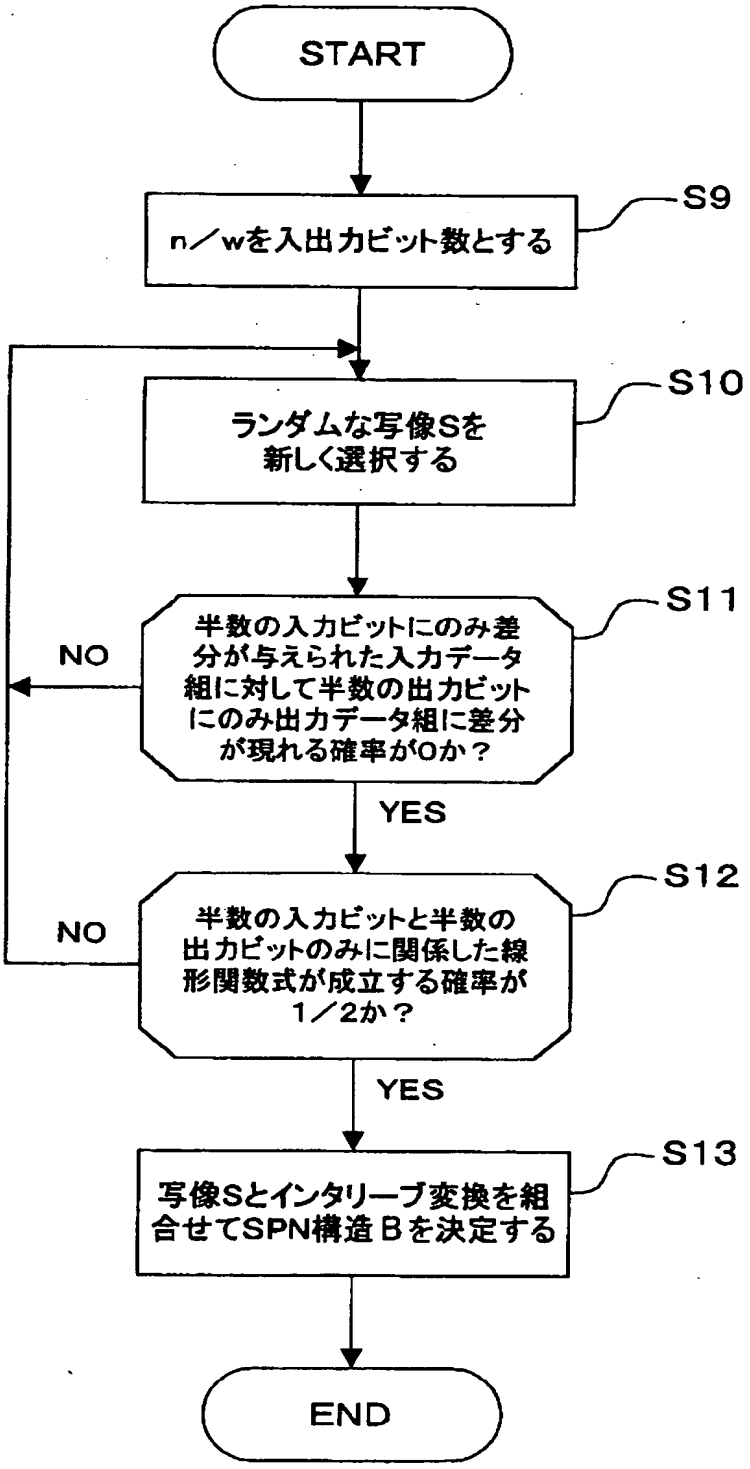
【図６】

Feiste1構造で用いられるF関数の例を示す図



【図７】

SPN構造決定処理の詳細フローチャート



【図８】

S関数に与えられる入力差分に対して
出力差分が現われる確率を説明する図

	出力差分					
入力差分	(0001)	(0010)	(0011)	(0100)	(1000)	(1100)
(0001)	0	0	0	2	2	0
(0010)	0	0	0	0	2	2
(0011)	0	0	0	2	0	2
(0100)	0	0	2	0	0	0
(1000)	2	0	4	0	0	0
(1100)	4	2	0	0	0	0

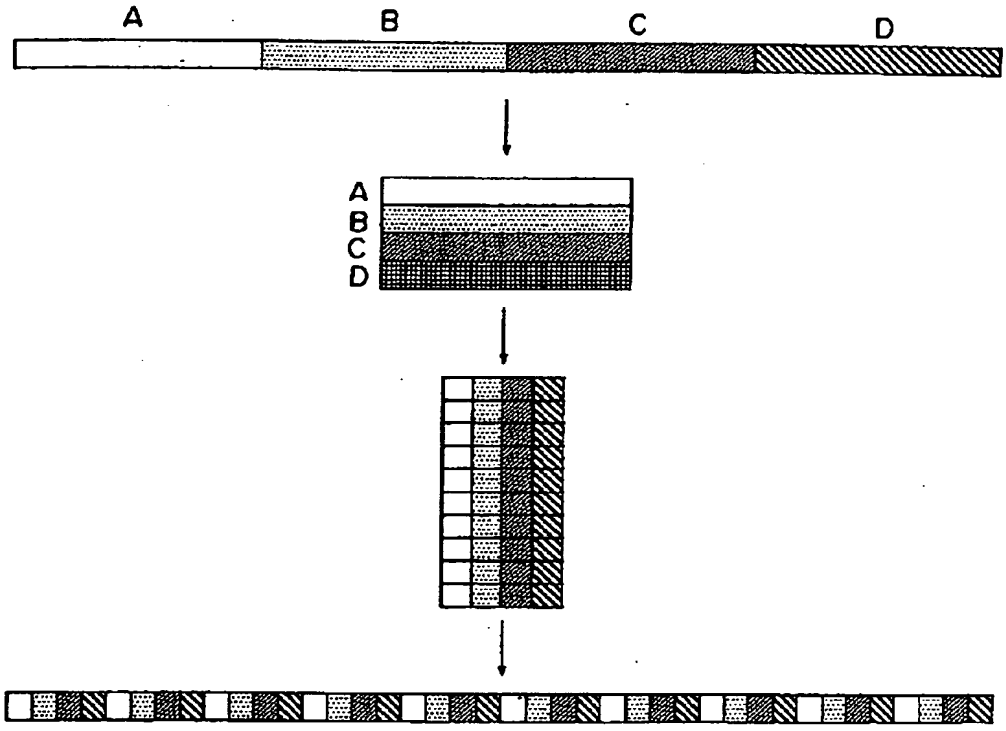
【図９】

S関数における入出力ビットの間の
線形関数式の成立確率を説明する図

入力ビット	出力ビット (0001)	(0010)	(0011)	(0100)	(1000)	(1100)
(0001)	0	0	0	-4	2	-2
(0010)	0	0	0	2	4	2
(0011)	0	0	0	-2	-2	0
(0100)	2	2	-4	0	0	0
(1000)	-2	-2	0	0	0	0
(1100)	0	4	0	0	0	0

【図１０】

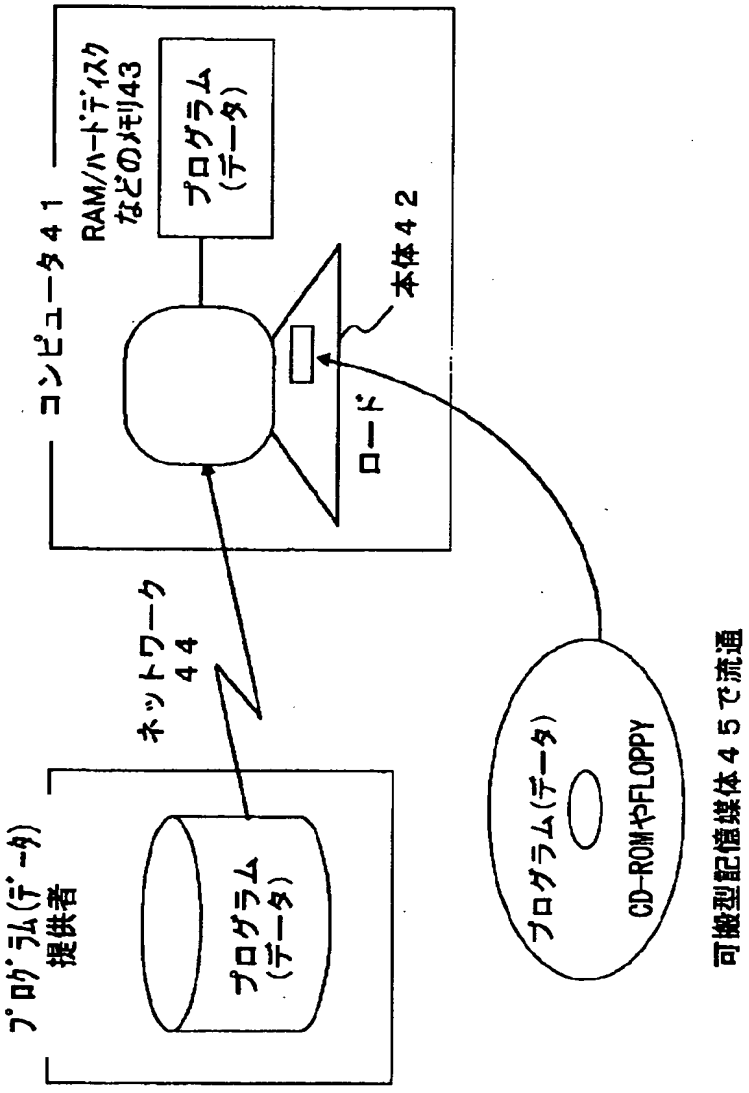
インタリーブ変換の例を説明する図



出証特２０００－３１０５８６９

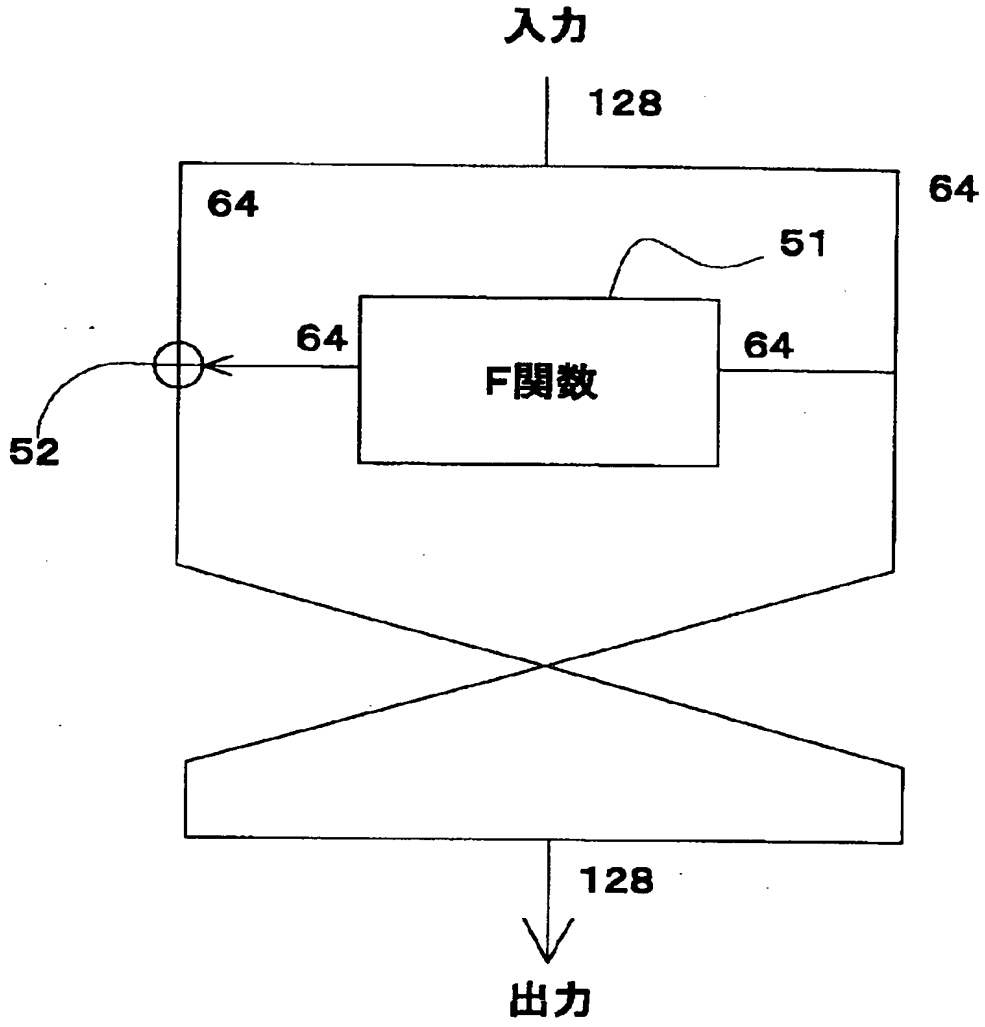
【図１１】

プログラムのコンピュータへの
ローディングを説明する図



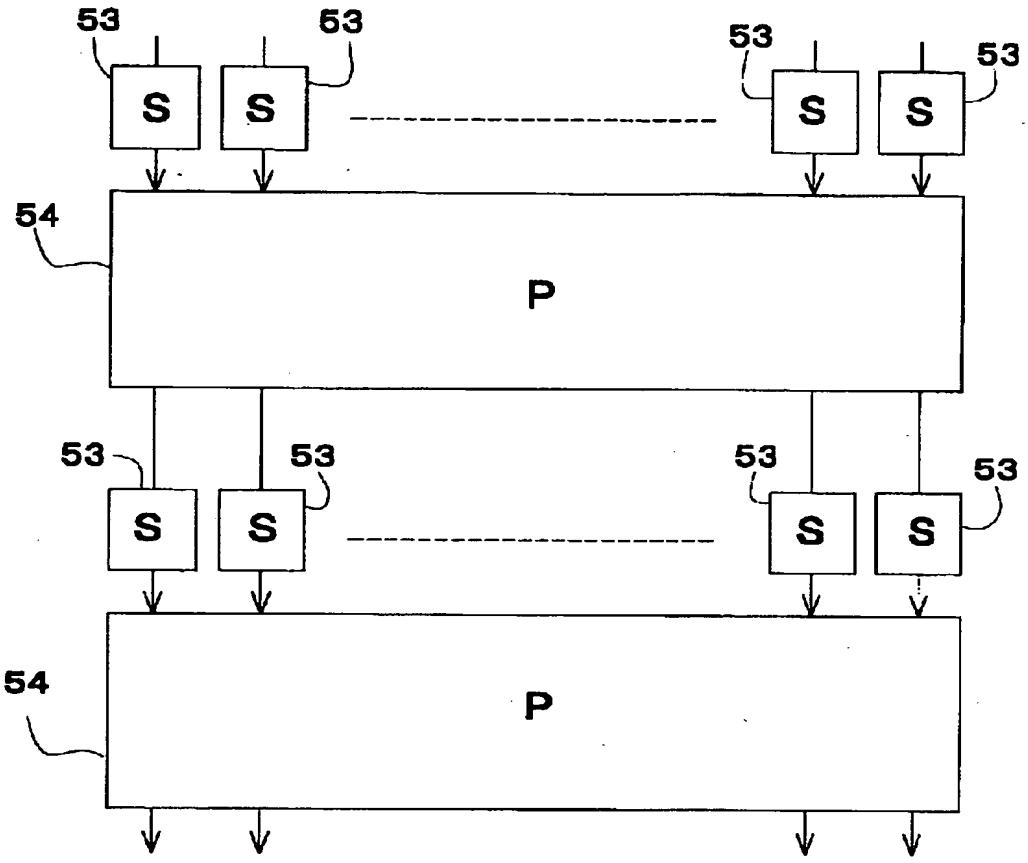
【図１２】

Feiste1構造の例を示す図



【図１３】

SPN構造の例を示す図



S:非線形変換、P:線形変換

【書類名】　　要約書

【要約】

【課題】　共通鍵ブロック暗号化方式において、演算量を削減させ、かつデータ拡散性能を向上させる。

【解決手段】　Feistel 構造を用いてデータ変換を行う手段２の１つ以上と、ＳＰＮ構造を用いてデータ変換を行う手段３の１つ以上とを、データ入力とデータ出力との間で縦続的に組み合わせる。またＳＰＮ構造内で、固定された半数の入力ビット、および同位置にある半数の出力ビットにのみ関係する線形関係式がすべての入出力データ間で成立する確率が１／２となる非線形変換手段を用いる。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社